Sophos veröffentlicht Kompendium zum IT-Security-Topthema Ransomware

Angriffsmethoden und Tipps zum Schutz vor den elf größten Ransomware-Familien, darunter WannaCry, SamSam, RobbinHood, Ryuk, MegaCortex.

Wiesbaden, 19. November 2019 – Sophos hat eine neue Ausgabe in seiner englischsprachigen Reihe der „Playbooks for Defenders" veröffentlicht. Mit dem Titel „How Ransomware Attacks" beschreiben die SophosLabs detailliert, wie unterschiedliche Ransomware-Varianten ihre Opfer angreifen und welche Vorsichtsmaßnahmen zum Schutz zu treffen sind. Das Kompendium richtet sich speziell an IT- sowie Security-Fachleute und ist eine Ergänzung zum jüngsten Sophos Threat Report 2020. Analysiert werden elf der gängigsten und beständigsten Ransomware-Familien, darunter Ryuk, BitPaymer und MegaCortex.

Detaillierte Einblicke in die Vorgehensweise der Kriminellen
Im neuesten Playbook for Defenders beschreiben die SophosLabs detailliert, wie Ransomware versucht, unbemerkt an der Security vorbeizuschlüpfen. Meist nutzen die Angreifer dafür vertrauenswürdige und legitime Prozesse, um dann über interne Systeme eine maximale Anzahl von Dateien zu verschlüsseln sowie Backup- und Wiederherstellungsprozesse zu deaktivieren, bevor ein IT-Sicherheitsteam einschreiten kann. Die wichtigsten Kapitel des Kompendiums umfassen:

Verbreitung
Ransomware wird typischerweise auf eine von drei Arten verteilt: Als Kryptowurm, der sich schnell auf andere Computer repliziert, um eine maximale Wirkung zu erzielen (z.B. WannaCry). Eine weitere Variante ist Ransomware-as-a-Service (RaaS), der verstärkt im Dark Web als Distributions-Kit verkauft wird (z.B. Sodinokibi). Die dritte Art der Verteilung erfolgt mittels eines automatisierten, aktiven gegnerischen Angriffs, bei dem Angreifer die Ransomware nach einem automatisierten Scan von Netzwerken für Systeme mit schwachem Schutz manuell einsetzen.

Kryptographisches Code Signing
Kryptographische Code Signing Ransomware mit einem gekauften oder gestohlenen legitimen Zertifikat versucht Sicherheitssoftware davon zu überzeugen, dass der Code vertrauenswürdig ist und keine Analyse benötigt.

Privilegien
Um Privilegien beziehungsweise Zugriffsrechte zu erhöhen, nutzen Angreifer leicht verfügbare Exploits wie EternalBlue. Auf diese Weise kann der Angreifer Programme wie Remote Access Tools (RATs) installieren, Daten anzeigen, ändern oder löschen sowie neue Konten mit vollen Benutzerrechten erstellen und Sicherheitssoftware deaktivieren.

Bewegung im Netz
Angreifer nutzen die seitliche Bewegung bei ihrer Jagd im Netzwerk nach Datei- und Backup-Servern, um die volle Wirkung des Ransomware-Angriffs zu entfalten. Dabei bleiben sie unter dem Radar, quasi unbemerkt. Innerhalb einer Stunde können Angreifer ein Skript

erstellen, um die Ransomware auf vernetzten Endpunkten und Servern zu kopieren und auszuführen.

Fernangriffe
Dateiserver sind oft nicht mit der Ransomware infiziert. Stattdessen läuft die Attacke typischerweise auf einem oder mehreren kompromittierten Endpunkten, wobei ein privilegiertes Benutzerkonto missbraucht wird Der Zugriff kann auch über das Remote Desktop Protocol (RDP) oder via Remote Monitoring and Management (RMM)-Lösungen erfolgen.

Dateiverschlüsselung und Umbenennung
Es existiert eine Reihe von unterschiedlichen Methoden zur Dateiverschlüsselung, einschließlich des einfachen Überschreibens des Dokuments. Die meisten Methoden werden durch das Löschen des Backups oder der Originalkopie ergänzt, um den Wiederherstellungsprozess zu verhindern.

Tipps zum Ransomware-Schutz
- Überprüfung, ob man über einen vollständigen Bestand aller mit dem Netzwerk verbundenen Geräte verfügt und ob alle Sicherheitssoftware-Lösungen, die man auf diesen Geräten verwendet, auf dem neuesten Stand ist.
- Installation der neuesten Sicherheitsupdates auf allen Geräten im Netzwerk.
- Patchen aller Computer gegen die von WannaCry verwendete EternalBlue-Schwachstelle.
- Regelmäßig Backups der wichtigsten und aktuellsten Daten auf einem Offline-Speicher.
- Administratoren sollten die Multi-Faktor-Authentifizierung auf allen Managementsystemen aktivieren, um zu verhindern, dass Angreifer Sicherheitsprodukte während eines Angriffs deaktivieren.
- Die Strategie eines mehrschichtigen Sicherheitsmodells ist die beste Vorgehensweise zur Vorbeugung.
- Geeignete Security-Lösungen: Sophos Intercept X bietet Schutz für Endgeräte, indem diverse Next-Generation-Technologien kombiniert werden, um Malware-Erkennung, Exploit-Schutz sowie eine Endpoint Detection and Response (EDR) bereitzustellen.

Das vollständige Playbook How Ransomware Attacks sowie ein ergänzender Artikel von SophosLabs, How the Most Damaging Ransomware Evades IT Security, sind unter folgenden Links verfügbar:
- Playbook How Ransomware Attacks: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-ransomware-behavior-report.pdf
- How the Most Damaging Ransomware Evades IT Security: https://news.sophos.com/en-us/2019/11/14/how-the-most-damaging-ransomware-evades-it-security/

Über Sophos
Als ein weltweit führender Anbieter von Next-Generation-Cybersicherheit schützt Sophos mehr als 400.000 Unternehmen jeder Größe in über 150 Ländern vor den neuesten Cyberbedrohungen. Mit den SophosLabs und seinem globalen Team für Bedrohungs- und Datenanalyse schützen die Cloud- und KI-gestützten Sophos-Lösungen Endpoints (Laptops, Server und mobile Geräte) sowie Netzwerke vor sich ständig verändernden Cyberangriffen, einschließlich Ransomware, Malware, Exploits, Datenexfiltration, individuellen Hackervorstößen, Phishing und mehr. Die cloud-basierte Plattform Sophos Central integriert über APIs das gesamte Next Generation Sophos-Portfolio, von der Intercept X Endpoint-Lösung bis zur XG Firewall, in einem einzigen Synchronized-Security-System. Sophos treibt die Entwicklung zur Next Generation Cybersicherheit voran und setzt fortschrittliche Technologien, beispielsweise aus den Bereichen Cloud, Machine Learning, APIs, Automatisierung oder Managed Threat Response ein, um Unternehmen jeder Größe Schutz der Enterprise-Klasse zu bieten. Sophos vertreibt Produkte und Services exklusiv über einen globalen Channel mit mehr als 47.000 Partnern und Managed Service Providern (MSP). Sophos stellt seine innovativen, gewerblichen Technologien auch Privatanwendern via Sophos Home zur Verfügung. Das Unternehmen hat seinen Hauptsitz in Oxford, Großbritannien, und ist an der Londoner Börse unter dem Symbol "SOPH" notiert. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de